IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF HAWAII

UNITED STATES OF AMERICA,

CR. NO. 17-00104 JMS-KJM

Plaintiff,

ORDER DENYING DEFENDANT'S MOTION FOR SANCTIONS, ECF NO. 845

VS.

LEIHINAHINA SULLIVAN,

Defendant.

ORDER DENYING DEFENDANT'S MOTION FOR SANCTIONS, <u>ECF NO. 845</u>

Before the court is pro se Defendant Leihinahina Sullivan's ("Defendant") Motion for Sanctions relating to the loss of evidence by the United States. ECF No. 845. For the reasons stated below, the court DENIES Defendant's Motion.

I. INTRODUCTION

The United States lost two iPhones and one thumb drive seized after the execution of a June 1, 2016 search warrant on Defendant's residence. *See* Mar. 13, 2020 Letter by the Government, ECF No. 884-4. Specifically, the United States cannot locate one iPhone belonging to Defendant ("iPhone #1"), one iPhone belonging to Defendant's husband ("iPhone #2"), and a thumb drive. *See id*. Defendant subsequently filed multiple motions seeking, in part, sanctions for the

loss of this evidence. *See* ECF No. 819 at PageID #8682. "[G]iven the confusion that Defendant has caused by her filing of multiple motions, many of which are repetitive and also address multiple issues," the court struck all of Defendant's pending motions and granted Defendant "leave to file one comprehensive motion for sanctions based on the Government's loss of electronic data." *Id.* (original emphasis omitted).

Pursuant to the court's order, Defendant filed her one comprehensive Motion for Sanctions on April 17, 2020. ECF No. 845. The United States filed its Opposition on May 11, 2020. ECF No. 884. Defendant filed her Reply on June 5, 2020. ECF No. 920.

The court held a hearing on July 17, 2020. Internal Revenue Service-Computer Investigative Specialist ("IRS-CIS") Special Agent Michael Hammond ("CIS Hammond") was the sole witness. He explained what was extracted from the two iPhones and thumb drive prior to their disappearance, and what is now available to the parties and the court to view and access. *See* ECF No. 975. On July 24, 2020, both parties submitted supplemental briefing. ECF Nos. 979, 980.

///

///

///

///

II. BACKGROUND

A. Seizure and Subsequent Loss of the iPhones and Thumb Drive

On June 1, 2016, the government seized iPhones #1 and #2, along with a thumb drive, pursuant to a search warrant executed on Defendant's residence. *See* ECF No. 884-1. On June 2, 2016, IRS-CIS Special Agent Jeff Jack ("CIS Jack"), 1 created a forensic image² of the thumb drive. Hammond Decl., ECF No. 884-2 at PageID #9009. Cellebrite extractions (a forensic tool, discussed in further detail below) were performed on the two iPhones. *Id.* at PageID #9010. Once the extractions of the cellphones and forensic imaging of the thumb drive were completed in June 2016, the chain of custody and/or the paper trail as to these three items ceased to exist. The government maintains that after his forensic work, CIS Jack made a notation on paperwork that the three items were returned to the "case agent," but no one can identify that particular case agent, CIS Jack has no

¹ At the time of his work on the investigation, CIS Jack was located in San Jose, California; he retired in or around January 2018. ECF No. 884-2 at PageID #9009. CIS Hammond is currently assigned to this case. *Id.* at PageID #9009-10.

² Per CIS Hammond, "[a] forensic image is a bit-by-bit, sector-by-sector copy of a physical storage device, such as a . . . USB Thumbdrive, including all files, programs, folders and unallocated, free and slack space. A forensic image is an exact copy of computer data without making changes to the original evidence." ECF No. 884-2 at PageID #9009.

³ The Assistant United States Attorney ("AUSA") stated during the July 17, 2020 hearing that it is unclear if CIS Jack was referring to some agent at the scene of the search or the actual case agent (and the case agent, IRS Criminal Investigation Division Special Agent Mark McPherson claims that he has no independent recollection of the two iPhones or the thumb drive). ECF No. 988 at PageID #10035-36.

independent recollection of what he did with the evidence, and the iPhones and thumb drive cannot be located in any of the IRS offices involved in the investigation.⁴ ECF No. 988 at PageID #10035-36. None of the "case agents" recalls receiving the electronic devices from CIS Jack. *Id.* at PageID #10036. Further, the government cannot locate any chain-of-custody logs pertaining to each missing item.

Accordingly, the government concedes that the "evidence logs" (meaning chain of custody logs) for these items are missing along with the items themselves. *Id.* at PageID #10043 ("THE COURT: Okay. So the evidence logs are lost also? [AUSA]: I – I guess that would be something that we would surmise, Your Honor."). The government further concedes that, in viewing the evidence in the light most favorable to Defendant, it is a "fair" "assumption" to conclude that the iPhones and thumb drive were lost as early as June 2016 after the extractions and imaging were completed. *Id.* at PageID #10114.

The government represents that at trial it will not use any of the information obtained from iPhone #1 or iPhone #2, and that it intends to use "limited information" obtained from the thumb drive. *Id.* at PageID #10040-41.

⁴ Defendant also alleges that two additional iPhones are missing. *See* ECF No. 845 at PageID #8805 (alleging that the government "Failed to Report Four (4) iPhone . . . Went Missing"). But Defendant provides no evidence in support of that claim, and the government has represented that it in fact possesses these other two iPhones. Given this record, the court construes Defendant's Motion for Sanction as limited to iPhones #1 and #2, and the thumb drive.

B. The Cellebrite Extractions of iPhones #1 and #2, and the Forensic Imaging of the Thumb Drive

CIS Hammond explained that the IRS uses Cellebrite, a forensic software tool, to extract data from seized cellphones. *Id.* at PageID #10050. The extraction does not create an exact image of the cellphone. Rather, particular information is "extracted" including "historical data on the phone such as call logs, contacts, text messages, pictures," "[e]-mail stored in [the] phone . . . , multimedia content, plus information to identify the phone." *Id.*; see also ECF No. 975-4 at PageID #9930-31 (screenshot of extraction summary of iPhone #2, showing the data extracted including SMS and MMS messages (text messages), voicemails, audio, images, and video files, chats, call log, contacts, and calendar, among other things).⁵ CIS Hammond further testified that text messages, for example, are unique to a cellphone, but e-mails are not unique to a cellphone because they run through a third-party application program like Google's e-mail application (commonly referred to as "gmail"). See ECF No. 988 at PageID #10056.6 Nevertheless, CIS Hammond explained that some e-mails may still be on the

⁵ CIS Hammond created four exhibits, all of which were introduced into evidence at the July 17, 2020 hearing: two extraction reports from iPhone #1, ECF No. 975-1 & -3; an extraction summary from iPhone #2, ECF No. 975-4; and a screenshot showing that iPhone #1 has partially encrypted information, which the government cannot access without Defendant's passcode, ECF No. 975-2.

⁶ See also United States v. Cano, 934 F.3d 1002, 1009-10 (9th Cir. 2019) ("A Cellebrite search enables the user to access text messages, contacts, call logs, media, and application data (continued . . .)

cellphone itself if these e-mails were "downloaded or saved or temporarily stored on phones for ease of access for the owner." *Id.* But "[t]hese days more often than not e-mails are not downloaded or stored [onto] phones . . . because they are stored on the . . . e-mail application server, not actually on the phone." *Id.* at PageID #10056-57.

Two extractions were conducted on iPhone #1, one on June 2 and the other on June 3, 2016. ECF No. 975-1 & -3; *see also* ECF No. 988 at PageID #10072. CIS Hammond explained that iPhone #1 was partially encrypted and partially unencrypted, and thus, he had to conduct two separate extractions—one on the encrypted portion and one on the unencrypted portion. ECF No. 988 at PageID #10069, 10071-72. Ultimately, CIS Jack was able to extract *and* obtain usable data from the unencrypted portion of iPhone #1, but the encrypted portion, although extracted, requires a passcode to access usable data. And, because the IRS never had access to the passcode, it was "not able to analyze the data that's contained within" that encrypted portion. *Id.* at PageID # 10069.8 CIS Hammond

on a cell phone It does not, however, allow the user to access data stored within third-party applications.").

⁷ It appears that a "logical extraction" was used on the unencrypted data and a "file system extraction" was used on the encrypted data. *See* ECF No. 988 at PageID #10058-59; ECF No. 979-2 at Page ID #9981-82.

⁸ Defendant, as is her absolute right, has not provided the government with the passcode to unlock the encrypted data on iPhone #1. ECF No. 781 at PageID #8443 n.1; ECF No. 979 at PageID #9966 n.5.

explained that the encrypted data on iPhone #1 could be accessed at the present time with the passcode—that is, even without access to iPhone #1 itself, the data can be accessed with the passcode using the Cellebrite encrypted extraction. *Id.* at PageID #10069-70. CIS Hammond believes that iPhone #1's encrypted information includes "contacts, call logs, more user account and user information." *Id.* at PageID #10062.

Although iPhone #2 was also encrypted, the government obtained the passcode from Defendant's husband. *See* ECF No. 979 at PageID #9966 n. 5. As a result, on June 3, 2016, usable data was extracted from iPhone #2. ECF No. 975-4.

CIS Hammond further explained that a Cellebrite extraction is not an exact image or replica of all the contents on a phone, and "it is possible that [the extraction does] not contain everything . . . that is on the physical phone." ECF No. 988 at PageID #10067. And it appears that approximately 5-7 gigabytes of data were not extracted from iPhone #1. ECF No. 979-2 at PageID #9981-82. CIS Hammond testified that information missing from the extraction could include third-party applications or games. ECF No. 988 at PageID #10067-68. But because "each phone is specific," CIS Hammond could not testify as to what specifically the Cellebrite extraction failed to extract from iPhone #1. *Id.* at PageID #10077.

Unlike the iPhones, CIS Jack created a complete forensic image—an exact copy of the electronic data—of the thumb drive. Hammond Decl. ¶¶ 4-5, ECF No. 884-2 at PageID #9009.

III. LEGAL STANDARD

In *California v. Trombetta*, 467 U.S. 479, 489, 104 S.Ct. 2528, 81 L.Ed.2d 413 (1984), the Supreme Court held that the government violates the defendant's right to due process if the unavailable evidence possessed exculpatory value that was apparent before the evidence was destroyed, and [is] of such a nature that the defendant would be unable to obtain comparable evidence by other reasonably available means. The Court subsequently added a third requirement for establishing a due process violation in *Arizona v. Youngblood*, 488 U.S. 51, 57-58, 109 S.Ct. 333, 102 L.Ed.2d 281 (1988), holding that the defendant must demonstrate that the government acted in bad faith in failing to preserve the potentially useful evidence.

United States v. Zaragoza-Moreira, 780 F.3d 971, 977 (9th Cir. 2015) (internal quotation marks and some citations omitted). Further, "[t]he presence or absence of bad faith turns on the government's knowledge of the apparent exculpatory value of the evidence at the time it was lost or destroyed, because without knowledge of the potential usefulness of the evidence, the evidence could not have been destroyed in bad faith." *Id.* "Bad faith requires more than mere negligence or recklessness." *United States v. Flyer*, 633 F.3d 911, 916 (9th Cir. 2011).

The burden is on Defendant to prove the due process violation. *United States v. Sivilla*, 714 F.3d 1168, 1172 (9th Cir. 2013).

Even absent a due process violation, the court may impose sanctions. "The rule governing sanctions for lost or destroyed evidence is found in the controlling concurrence in *United States v. Loud Hawk*, 628 F.2d 1139 (9th Cir. 1979) (en banc) (Kennedy J., concurring), reversed on other grounds in United States v. W.R. Grace, 526 F.3d 499, 506 (9th Cir. 2008)." United States v. Robertson, 895 F.3d 1206, 1213 (9th Cir. 2018). "If the government destroys evidence under circumstances that do not violate a defendant's constitutional rights, the court may still impose sanctions including suppression of secondary evidence." Flyer, 633 F.3d at 916 (citing Loud Hawk, 628 F.2d at 1152). "The proper balance is that between the quality of the Government's conduct and the degree of prejudice to the accused. The Government bears the burden of justifying its conduct and the defendant bears the burden of demonstrating prejudice." Loud Hawk, 628 F.2d at 1152 (citing *United States v. Mays*, 549 F.2d 670, 677, 678 (9th Cir. 1977) (Kennedy J., concurring).

IV. <u>DISCUSSION</u>

Defendant does not appear to dispute that a full forensic image was made of the thumb drive, or otherwise argue that there was potentially exculpatory evidence contained on the thumb drive that is now missing. And Defendant has

made no specific allegations that iPhone #2 contains any missing evidence, exculpatory or otherwise. Instead, Defendant argues that iPhone #1 has missing text messages and e-mails, those texts and e-mails are exculpatory, and the government acted in bad faith. The court thus limits its analysis to iPhone #1, and determines that Defendant has failed to meet her burden to show that iPhone #1 possessed exculpatory text messages or e-mails that was apparent before it was lost, that the government acted in bad faith, or that Defendant would not be able to obtain comparable evidence by other reasonably available means.⁹

A. Defendant Has Not Shown that iPhone #1 Contained Potentially Exculpatory Evidence That Was Apparent to the Government at the Time it was Lost¹⁰

Defendant argues that iPhone #1 contained text messages and e-mails that she never received through discovery¹¹ and that these text messages and e-mails contain exculpatory communications between herself and others. ECF No.

⁹ Although the court limits its analysis to iPhone #1, the analysis and conclusion set forth below applies equally to iPhone #2 and the thumb drive.

As discussed above, it is not entirely clear *when* the government lost the iPhones and thumb drive. The evidence is clear, however, that there is no record of the IRS having the iPhones and thumb drive after the June 2016 forensic examination by CIS Jack. Thus, the record certainly supports a reasonable inference that the evidence was lost shortly after CIS Jack possessed the evidence in June 2016. But even if the IRS lost the evidence sometime after June 2016, but before the government began its attempt to locate the evidence in March 2020, the court's analysis would be the same.

¹¹ The Cellebrite extractions were provided to Defendant in discovery on January 17, 2020. *See* ECF 729-1 at PageID #7915, 7922.

988 at PageID #10107 ("It was apparent [that iPhone #1 contained exculpatory evidence] because that was information that I never received in discovery."); see also ECF No. 980 at PageID #9996. But missing evidence alone does not make it potentially "exculpatory." And Defendant's conclusory assertion, made only after she learned that iPhone #1 was missing, that iPhone #1 contained exculpatory text messages and e-mails is merely that—conclusory. 12 In fact, based on the evidence before the court, any text messages or e-mail communications that Defendant had with alleged victims and/or witnesses is as likely to incriminate Defendant as exculpate her. See United States v. Drake, 543 F.3d 1080, 1090 (9th Cir. 2008) (explaining that "[t]he exculpatory value of an item of evidence is not 'apparent' when the evidence merely 'could have' exculpated the defendant" (citing Youngblood, 488 U.S. at 56), and finding that the missing digital recording was "far from clearly exculpatory" because it was "possible that it would have further incriminated [the defendant]").

¹² Defendant cites to various transcripts and filings, including a February 2, 2018 filing regarding her bail status (ECF No. 82), in an attempt to show that she had previously made clear that iPhone #1 contained exculpatory evidence. *See* ECF No. 980 at PageID #9992-94. But Defendant simply cites to various times that she reasserted her defense and/or raised discovery issues; none of these transcripts or filings shows that Defendant had identified iPhone #1 as containing exculpatory evidence *before* she was notified by letter dated March 13, 2020 that the two iPhones were missing. For example, Defendant filed two motions seeking return of both iPhone #1 and iPhone #2, one on December 3, 2019 and one on March 11, 2020, yet neither of these motions mentions that iPhone #1 contains exculpatory evidence. *See* ECF Nos. 403, 729.

Here, the application for a search warrant on Defendant's residence relied on text messages exchanged between Defendant and a witness. *See* ECF No. 357-1 at PageID #3650. Thus, because the purported e-mails and text messages on iPhone #1 (based on the evidence before the court) were as equally likely to be incriminating as exculpatory, any such exculpatory value of that data on iPhone #1 could not have been readily apparent to the government at the time iPhone #1 was lost in June 2016 or thereafter.

B. Defendant Has Not Shown that the Government Acted in Bad Faith

Because Defendant has failed to show that any of iPhone #1's electronic data contained potentially exculpatory evidence, it follows that she has not shown that the government acted in bad faith. As the Ninth Circuit has explained, the "bad faith requirement dovetails" with the requirement "that the exculpatory value of the evidence be apparent before its destruction." *United States v. Cooper*, 983 F.2d 928, 931 (9th Cir. 1993) (citing *Trombetta*, 467 U.S. at 489). "The presence or absence of bad faith turns on the government's knowledge of the apparent exculpatory value of the evidence at the time it was lost or destroyed, because without knowledge of the potential usefulness of the evidence, the evidence could not have been destroyed in bad faith." *Zaragoza-Moreira*, 780 F.3d at 977 (citing *Youngblood*, 488 U.S. at 56 n.*). Thus, because Defendant has not shown that iPhone #1 had potentially exculpatory value, let alone that any

exculpatory value was apparent to the government at the time it was lost, the government's mere loss of iPhone #1 could not have been in bad faith.

Indeed, the IRS has been *negligent* in losing the electronic data—something it concedes. It greatly concerns the court that the IRS would be so careless and cavalier in handling property which it is entrusted to safeguard and maintain. As CIS Hammond testified, after the iPhones and thumb drive were extracted and forensically imaged, they simply vanished. But such carelessness, without more, does not amount to bad faith by the government.¹³

C. Defendant Has Not Shown that the Text Messages and E-Mails Cannot be Obtained Through Alternative Reasonable Means

Even if Defendant had shown that iPhone #1 contained potentially exculpatory text messages and/or e-mails (which she has not), she has not shown

The court fully recognizes that this is not the first time in this case where the government has been negligent or sloppy during its investigation. *See, e.g.*, ECF No. 824 at PageID #8721-22 (noting that the government's taint team process was deficient because privileged materials were sent by a taint team to the prosecution team, but there was no prejudice to Defendant because these files were never viewed by the prosecution team); *see also id.* at PageID #8700-02, 16 (noting that the government indicated it had seized "Lexus Nexus" documents but the government could not locate these documents). Nonetheless, and to be clear, based on the evidence presented, the court does not find that the government *intentionally* lost or destroyed the iPhones or thumb drive (and their respective chain-of-custody logs). There is simply no evidence that anyone within the IRS sought to have certain evidence destroyed, or otherwise had any reason to destroy the evidence. At most, the government has shown, several times, an unfortunate sloppiness in several parts of the investigation. The court expects better—much better—from the government.

that comparable evidence could not be obtained by other reasonably available means.

First, Defendant has provided no evidence to show that the extraction reports failed to capture the text messages or e-mails that she claims are missing from the discovery productions. At most, Defendant alleges that some text messages and emails are missing from discovery provided to her. But the mere fact that some text messages and/or e-mails may be missing in discovery materials (separate from the discovery extracted from the iPhones and thumb drive)¹⁴ does not establish that they are not in the data extracted from iPhone #1.¹⁵

And if any missing text messages or email are in the encrypted extraction from iPhone #1, Defendant, not the government, holds the keys to the encrypted extraction from iPhone #1. That is, even if any missing text messages

And to be clear, the court is not finding that these texts and/or e-mails were not produced in discovery. Other than conclusory assertions from Defendant that these e-mails were not produced, she has not provided evidence that she has reviewed the discovery produced to confirm that these e-mails were missing in the discovery. *See*, *e.g.*, ECF No. 979 at PageID #9971 (government's brief noting that "substantial amounts of e-mail involving the defendant were turned over in discovery found on the Apple Desktop seized in the June 2016 residential search warrant, the 2019 iCloud search warrant, and other sources"). But the court also acknowledges the difficulty of proving the *absence* of something and also recognizes that the government has not identified the production of some these e-mails Defendant identified in her filing at ECF No. 82. *See* ECF No. 988 at PageID #10110-11 (the government noting it had "not analyzed" the unencrypted portions of iPhone #1).

¹⁵ In fact, CIS Hammond testified that text messages are typically the types of information that is extracted from phones. ECF No. 988 at PageID #10050; *see also* ECF No. 975-4 at PageID #9930 (noting on iPhone #2 (unencrypted phone) containing SMS Messages of "2444 (80)" and MMS messages of "212 (23)"). Again, Defendant has provided no evidence other than her conclusory speculation that the extraction of the text messages was incomplete.

and e-mails are contained solely in the encrypted extraction (and not in the unencrypted extraction, or in the other discovery productions including data from Defendant's desktop computer), the government cannot access that data without Defendant's passcode. And Defendant cannot both refuse to provide the passcode required to access iPhone #1's encrypted information and simultaneously claim that the information is unavailable to her. To be clear, Defendant is under no obligation to provide the government with the passcode to iPhone #1; but she cannot complain that the government is withholding information from her when she alone is able to provide a passcode to access that very information.

Accordingly, Defendant has not shown that the alleged missing text messages and e-mails are unavailable from the extraction reports.

Second, even if Defendant had shown that the alleged missing text messages and/or e-mails were available solely on the physical iPhone #1 and were not extracted (which she has not), her argument *still* fails. She has not shown that she cannot obtain these e-mails and text messages through other reasonably available means. As to the text messages, CIS Hammond determined that iPhone #1 and iPhone #2 were "backed up to the iCloud within one day of the June 1, 2016 search warrant." Hammond Decl., ECF No. 979-2 at PageID #9982. And, according to Apple, iCloud backup includes iMessages and MMS/SMS messages. *Id.* And e-mail is not specific to a physical phone but rather can be accessed

through a third-party application like Google. Although Defendant claims she cannot access her gmail account because she does not remember her password, her mail account got "shut down," and that she "asked" Roadrunner and was told that Roadrunner does not save e-mails as far back as 2016, ECF No. 988 at PageID #10108, she admits that she has not tried to subpoena either Google (for gmail) or Roadrunner for these records. 16

///

///

///

///

///

///

///

///

///

///

¹⁶ The court is unaware if Defendant's e-mails (gmail or Roadrunner) are in fact available through legal process. But Defendant claims that the e-mails are unavailable to her without even having *attempted* any legal process. It is not sufficient to simply claim that the e-mails are unavailable without showing that reasonable effort was made to obtain the e-mails through legal process.

V. CONCLUSION

For the foregoing reasons, the court DENIES Defendant's Motion for

Sanctions for the loss of electronic data. ECF No. 845.¹⁷

IT IS SO ORDERED.

DATED: Honolulu, Hawaii, September 4, 2020.



/s/ J. Michael Seabright
J. Michael Seabright
Chief United States District Judge

United States v. Sullivan, Cr. No. 17-00104 JMS-KJM, Order Denying Defendant's Motion for Sanctions, ECF No. 845

uarrant." ECF No. 988 at PageID #10105; see also ECF No. 845 at PageID #8805, 8808 (seeking dismissal of Fourth Superseding Indictment because "nothing from the first search warrant should be used"); ECF No. 980 at PageID #9999. Because Defendant has not shown there was a due process violation or that she has been prejudiced from the missing devices (and their chain-of-custody logs), such sanction is unwarranted and would be vastly disproportionate to the government's negligence. Flyer, 633 F.3d at 916 (affirming district court's order declining to dismiss counts in indictment because there was no evidence of bad faith and no due process violation); see also ECF No. 824 at PageID #8723-24 (declining to suppress all the evidence obtained from the June 1, 2016 search warrant because such sanction was overly broad given that Defendant was not prejudiced, but agreeing that a lesser sanction of suppressing 473 files was appropriate). Further, Defendant has not suggested, let alone sought, any lesser sanction. See Loud Hawk, 628 F.2d at 1152 (citing United States v. Mays, 549 F.2d 70, 677, 678 (9th Cir. 1977) (Kennedy J., concurring); Robertson, 895 F.3d at 1213-14. And given the record before the court it is not clear that any specific lesser sanction would be appropriate.